IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL INC., a California corporation, Plaintiff, v. INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, SYMANTEC CORPORATION, a Delaware corporation, and INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, Defendants.	Civ. No. 04-1199-SLR

John F. Horvath, Esquire and Kyle Wagner Compton, Esquire of Fish & Richardson P.C., Wilmington, Delaware. Of Counsel: Howard G. Pollack, Esquire and Katherine D. Prescott, Esquire of Fish & Richardson P.C., Redwood City, California. Counsel for Plaintiff.

Richard L. Horwitz, Esquire and David Ellis Moore, Esquire of Potter Anderson & Corroon LLP, Wilmington, Delaware. Of Counsel: Holmes J. Hawkins III, Esquire and Natasha H. Moffitt, Esquire of King & Spalding LLP, Atlanta, Georgia. Theresa A. Moehlman, Esquire and Bhavana Joneja, Esquire of King & Spalding LLP, New York, New York. Counsel for Defendants INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation and INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation.

Richard K. Hermann, Esquire and Mary B. Matterer, Esquire of Morris, James, Hitchens & Williams, LLP, Wilmington, Delaware. Of Counsel: Lloyd R. Day, Jr., Esquire, Robert M. Galvin, Esquire, and Paul S. Grewal, Esquire of Day, Casebeer Madrid & Batchelder LLP, Cupertino, California. Michael J. Schallop, Esquire of Symantec Corporation, Cupertino, California. Counsel for Defendant SYMANTEC CORPORATION.

MEMORANDUM OPINION

Dated: October 17, 2006
Wilmington, Delaware

Sue L. Robinson
ROBINSON, Chief Judge

I. INTRODUCTION

Plaintiff SRI International, Inc. ("SRI") brought suit against defendants Symantec Corporation ("Symantec") and Internet Security Systems, Inc.[1] ("ISS") charging infringement of four patents: United States Patent Nos. 6,484,203 ("the '203 patent"), 6,708,212 ("the '212 patent"), 6,321,338 ("the '338 patent"), and 6,711,615 ("the '615 patent").[2]

Currently before the court are the defendants' motions for summary judgment of non-infringement. The court has jurisdiction over these matters pursuant to 28 U.S.C. § 1338(a). For the reasons that follow, Symantec's motion (D.I. 286) shall be granted in part and denied in part. ISS's motion, as it relates to non-infringement (D.I. 291), shall be denied.

II. BACKGROUND

Computers are used to process and store information, some of it sensitive in nature. Once computers are made part of a network, the information shared over the network is vulnerable to

[1] There are two defendants sharing the name "Internet Security Systems, Inc.," one a Delaware corporation and one a Georgia corporation. For purposes of this opinion, they shall collectively be referred to as "ISS".

[2] SRI has accused Symantec of infringing: '203 patent, claims 1-9, 11-20, 22; '212 patent, claims 1-11, 13-22, 24; '338 patent, claims 1-2, 4, 11-13, 18-19, 24; and '615 patent, claims 1-10, 12-21, 23, 34-41, 43-51, 53. SRI has accused ISS of infringing: '203 patent, claims 1-2, 4-6, 12-13 and 15-17; '338 patent, claims 1, 4, 5, 11-13, 18, 19 and 24; and '615 patent, claims 1-2, 4-6, 13-14 and 16-18.

unauthorized access by "intruders" (an "attack"). The field of invention of the patents in suit is intrusion detection.

A. The Patents in Suit[3]

The patents in suit relate to the monitoring and surveillance of computer networks for intrusion detection. In particular, the patents in suit teach a computer-automated method of hierarchical event monitoring and analysis within an enterprise network that allows for real-time detection of intruders. Upon detecting any suspicious activity, the network monitors generate reports of such activity. The claims of the '203 and '615 patents focus on methods and systems for deploying a hierarchy of network monitors that can generate and receive reports of suspicious network activity.

To detect attacks which do not possess deterministic signatures or to detect previously unknown (new) attacks, the patents in suit disclose the use of statistical detection methods on network data. The claims of the '338 patent are directed to a particular statistical algorithm for detecting suspicious network activity. The claims of the '212 patent combine both the use of statistical detection methods and a hierarchical architecture of network monitors.

B. The Accused Products

[3] The patents in suit claim priority from the same application, share almost identical written descriptions, and all issued without any office actions, rejections, or amendments.

Symantec is in the business of selling network intrusion detection systems ("NIDS"). SRI has identified two groups of Symantec products as infringing. The first group includes Man-Hunt 3.0 software, Symantec Network Security ("SNS") 4.0 software, SNS 7100 Series security appliances, and iForce Series appliances ("the ManHunt Products"). SRI has accused the ManHunt Products of infringing all four patents in suit.

The second group comprises the combination of Symantec Gateway Security ("SGS") products, including the SGS 1600, 5400 and 5600 series of security appliances, with management products - Symantec Incident Manager 3.0 ("IM") and Symantec Security Information Manager 9500 ("SIM") series of management appliances.[4] SRI has accused SGS 5400 Series products when used in combination with one of the Manager Products as infringing the asserted claims of the '203, '212 and '615 patents. SRI has accused the SGS 5600 and 1600 Series when used in combination with one of the Manager Products as infringing the asserted claims of the '203 and '615 patents (except claim 7 of the '615 patent).

[4] Symantec argues that SRI has failed to adduce sufficient evidence to prove either direct or contributory infringement of the '203, '212 and '615 patents based on combinations of the accused SGS and management products. The court finds, however, that there are genuine issues of material fact in this regard. Apparatus claims require no actual deployment. Moreover, there is circumstantial evidence of record of actual deployment. (See, e.g., D.I. 334, ex. R at SYM_P_0368994)

ISS also is in the business of selling NIDS. SRI accuses the configuration of ISS Sensors[5] operating in combination with SiteProtector SecurityFusion Module 2.0 ("Fusion") of infringing the '203 patent and the '615 patent. SRI also accuses the Proventia Anomoly Detection System ("ADS") operating in Standalone Mode of infringing the '338 patent.

III. STANDARD OF REVIEW

A. Summary Judgment

A court shall grant summary judgment only if "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). The moving party bears the burden of proving that no genuine issue of material fact exists. See Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 586 n.10 (1986). "Facts that could alter the outcome are 'material,' and disputes are 'genuine' if evidence exists from which a rational person could conclude that the position of the person with the burden of proof on the disputed issue is correct." Horowitz v. Fed. Kemper Life Assurance Co., 57 F.3d 300, 302 n.1 (3d Cir. 1995) (internal citations omitted). If the moving party has demonstrated an

[5] The ISS Sensors include RealSecure sensors (Network Sensor, Guard, Server Sensor and Desktop) and Proventia sensors (A, G, M, Server and Desktop).

absence of material fact, the nonmoving party then "must come forward with 'specific facts showing that there is a genuine issue for trial.'" Matsushita, 475 U.S. at 587 (quoting Fed. R. Civ. P. 56(e)). The court will "view the underlying facts and all reasonable inferences therefrom in the light most favorable to the party opposing the motion." Pa. Coal Ass'n v. Babbitt, 63 F.3d 231, 236 (3d Cir. 1995). The mere existence of some evidence in support of the nonmoving party, however, will not be sufficient for denial of a motion for summary judgment; there must be enough evidence to enable a jury reasonably to find for the nonmoving party on that issue. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 249 (1986).

B. Infringement

A patent is infringed when a person "without authority makes, uses or sells any patented invention, within the United States . . . during the term of the patent." 35 U.S.C. § 271(a). A court should employ a two-step analysis in making an infringement determination. Markman v. Westview Instruments, Inc., 52 F.3d 967, 976 (Fed. Cir. 1995). First, the court must construe the asserted claims to ascertain their meaning and scope. Id. Construction of the claims is a question of law subject to de novo review. See Cybor Corp. v. FAS Techs., 138 F.3d 1448, 1454 (Fed. Cir. 1998). The trier of fact must then compare the properly construed claims with the accused infringing product. Markman, 52 F.3d at 976. This second step is a question of fact. See Bai v. L & L Wings, Inc., 160 F.3d 1350, 1353 (Fed. Cir. 1998). Literal infringement occurs where each limitation of at least one claim of the patent is found exactly in the alleged infringer's product. Panduit Corp. v. Dennison Mfg. Co., 836 F.2d 1329, 1330 n.1 (Fed. Cir. 1987). An accused product that does not literally infringe a claim may still infringe under the doctrine of equivalents if each limitation of the claim is met in the accused product either literally or equivalently. See Sextant Avionique, S.A. v. Analog Devices, Inc., 172 F.3d 817, 826 (Fed. Cir. 1999). Occasionally, "the issue of literal infringement may be resolved with the step of claim construction, for upon correct claim construction, it may be apparent whether the accused device is within the claims." Multiform Desiccants, Inc. v. Medzam, 133 F.3d 1473, 1476 (Fed. Cir. 1998). The patent owner has the burden of proving infringement and must meet its burden by a preponderance of the evidence. SmithKline Diagnostics, Inc. v. Helena Lab. Corp., 859 F.2d 878, 889 (Fed. Cir. 1988) (citations omitted).

IV. DISCUSSION

A. The '203 Patent

Claim 1 of the '203 patent is a representative claim which discloses:

> A computer-automated method of hierarchical event monitoring and analysis within an enterprise network

> comprising:
> deploying a plurality of network monitors in the enterprise network;
> detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};
> generating, by the monitors, reports of said suspicious activity; and
> automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

('203 patent, col. 14, ll. 19-35)

Both Symantec and ISS contend in their motions that their accused products do not meet the "network monitor" limitation of the '203 patent. The court has construed "network monitor" to mean "[s]oftware and/or hardware that can collect, analyze and/or respond to data." (D.I. 468 at 2) Under the court's claim construction, the accused products meet the "network monitor" limitation. (See D.I. 287 at 30-31; D.I. 300 at 20-21)

ISS also argues that its accused products do not meet the "automatically receiving and integrating reports of suspicious activity" limitation. The court construed the "integrating" limitation to mean, "[w]ithout user intervention, receiving reports of suspicious activity and combining those reports into a different end product; i.e., something more than simply reiterating data." (D.I. 468 at 4) The court finds that there is a genuine issue of material fact with respect to this limitation. The record demonstrates that ISS's Fusion: (1) "**[c]ombin[es]** related IDS events **into** attack patterns to provide higher-level information on attacker intent" (D.I. 336, ex. Q at ISS00535786) (emphasis added); (2) the "Attack Pattern component ['APC'] uses a stored database procedure **to create** a site filter (or 'Incident') in the Database. A site filter is a collection of criteria that group together different rolled-up event data. If subsequent events meet one of the minimum requirements for the attack pattern, the Attack Pattern component updates the site filter in the Database" (D.I. 296 at 6) (emphasis added); and (3) "Attack Correlation consists of displaying on the SiteProtector Incident Console an **incident grouping that consolidates** a number of Sensor events sharing the event name and/or the IP addresses reported in the event" (D.I. 336, ex. E at 11)(emphasis added). The court cannot tell from the record whether the Attack Pattern component of the accused Fusion product simply combines and reiterates data, or whether it manipulates data in some fashion to create an end product different from the inputted data. Therefore, the court will deny ISS' motion for summary judgment in this regard.[6]

[6] Although ISS argued in its opening brief that SRI could not show direct infringement of the hierarchical claims, ISS apparently concedes, consistent with SRI's arguments in response, that the asserted apparatus claims can be infringed so long as Fusion APC is capable of performing the required functions.

B. The '212 Patent[7]

SRI has accused Symantec's SGS 5400 Series and ManHunt products of infringing the asserted claims of the '212 patent. Claim 1, a representative claim, discloses a

> [m]ethod for monitoring an enterprise network, said method comprising the steps of:
> deploying a plurality of network monitors in the enterprise network;
> detecting, by the network monitors, suspicious network activity based on analysis of network traffic data, wherein at least one of the network monitors utilizes a statistical detection method;
> generating, by the monitors, reports of said suspicious activity; and
> automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

('212 patent, col. 15, ll. 2-15)

The limitation in dispute is "statistical detection method." The court has construed this limitation to read "[a] method of detecting suspicious network activity by applying one or more statistical functions in the analysis of network traffic data. This method is not a signature matching detection method." (D.I. 468 at 6) The court finds there are genuine issues of material fact as to this limitation. The record demonstrates that: (1) "ManHunt uses counter-based and **statistical methods** to detect flood (denial of service) attacks . . ." (D.I. 334, ex. C at SYM_P_0049769) (emphasis added); and (2) in addition to "Protocol Anomaly Detection (PAD)" and "Stateful signatures", "ManHunt

[7] And claim 7 of the '615 patent.

sensors also incorporate a **statistical** or rate counter component to identify traffic shapes that indicate DDoS or flooding attacks" (D.I. 334, ex. D at SYM_P_0531466) (emphasis added). These product descriptions are sufficient to withstand Symantec's motion for summary judgment.

C. The '338 Patent

Claim 1 of the '338 patent, a representative claim, discloses:

> A method of network surveillance, comprising:
> receiving network packets handled by a network entity;
> building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;
> comparing at least one long-term and at least one short-term statistical profile; and
> determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

('338 patent, col. 14, ll. 62 to col. 15, ll. 5)

The only Symantec products accused of infringing the '338 asserted claims are the ManHunt products and, in particular, the "Flowchaser subsystem." (D.I. 266, ex. F at 14)[8] In his expert

[8] According to Dr. Kesidis, "ManHunt's Flowchaser subsystem communicates with network infrastructure components, such as routers and switches, as well as with ManHunt sensors, to collect data regarding network connections and network data transfers. The Flowchaser subsystem generates long-term statistical profiles regarding, for example, volumes of data transferred, numbers of network connections, and connection source and destination data. Flowchaser then generates short-term statistical profiles reflecting the same statistical measures, but over a shorter period of time. The Flowchaser subsystem generates a Flow Alert if the short-term profile differs significantly from the long-

report, Dr. Kesidis devotes one paragraph to literal infringement:

> The ManHunt Group of products build the claimed statistical profiles as part of its generation of "netflow alerts." Software processes within the ManHunt software receive packet data from one of the plurality of sensors of a ManHunt node. This packet data is used to derive "netflow statistics" that are maintained in a data store. These statistics include measures that monitor at least network connections. The ManHunt process accumulates the statistics in its data store for some period of time in order to establish a statistical baseline of activity associated with that measure. The process also develops shorter-term profiles of the same activity which it maintains in a separate data structure corresponding to the short-term profile.

(Id. at 72)

In support of his analysis, Dr. Kesidis references a single document of record, SYM_P_0136906-0136907, as well as selected portions of source code. The document is characterized as an "Architecture / Process List." The referenced pages describe the responsibilities of the "FDS (Flow Datastore)" as follows:

> The database of flow information collected by SNS sensors or Cisco routers. There exists a single database on each sensor node that has visibility into all flow data received by the node. All flow data is only stored in memory. Data is stored up to a maximum size. After the max size is reach[ed], flow data is removed based upon age.
>
> - maintains a history of recent flows
> - generates flow export snapshots upon request

term profile, for example, in the case of an inordinately high level of traffic." (D.I. 266, ex. F at 14)

(D.I. 334, ex. T at SYM_P_0136906) The FDS has three "external interfaces": One that "receives flow data from SNS sensors over UDP socket;" a second that "receives Netflow V5 data from Cisco routers over a UDP socket;" and a third to "access the file system to produce flow snapshots upon request from the manager command server." (Id. at SYM_P_ 0136906-0136907) Also included in the record is the "FlowChaser Data Store (FDS) Specification," where the FDS is described as "another data source from which ManHunt will accept information for its analysis and correlation engine. The FDS receives information about network flows from various devices (Cisco/Juniper routers, the sniffer, etc.) and stores the data in an optimized fashion to allow accelerated trackback, DoS protection, and advanced responsive actions." (D.I. 334, ex. W at SYM_P_0138243) The FDS has "two interfaces. One for the collection of flow data, and another to allow access to the stored flow data." (Id. at SYM_P_0138244) With respect to the design of FDS,

> [t]he data store itself is a very complex structure composed of mrii (memory resident ip index; a hybrid radix-4 tree and linked list data store), gcll (garbage collection linked list; a linked list kept in the order of what flows were least recently active), and individual flow records with "cookies" into each of these data stores to support the efficient destruction of the entries when they expire. The "cookies" are things like pointers to the individual list nodes so that things can be garbage collected without searching the entire list. . . .
>
> The data structure was chosen to minimize insertion time, and to enable inexpensive search for flows based

> on absolute or netmask-based criteria, as well as to be able to determine the overall network traffic that meets ip & mask combinations relatively cheaply. This data structure manages near-linear insertion time (including the cost of garbage collection as well) and logarithmic search times on the above mentioned characteristics.
>
> Basically, everything points to everything so that you can search and find a record in any way and then delete it if needs be.

(Id. at SYM_P_138245) Finally, FDS was described as "a long lived process and should not leak memory or crash." (Id. at SYM P_0138244) Based on these documents, Dr. Kesidis concludes that the "FDS flow data represents the long-term statistical profile," while the "flow snapshots" represent the short-term statistical profile. (D.I. 288, ex. G (ex. F at 2))

The court construed the "statistical profile" limitation as "[g]enerating at least two separate data structures, one a statistical description representative of historical network activity, and one a statistical description of recent network activity, where the statistical descriptions are based on at least one measure of the network packets and are generated through the use of statistical analysis; i.e., something more than simply collecting and retrieving data." (D.I. 468 at 5) Although broadly construed, the court does not believe that the limitation properly encompasses the FDS function as described in the documents, as the phrase "statistical profile" has been construed to require more than that raw data has been stored in memory over time and can be discretely searched. There is no persuasive evidence of record that the FDS generates two "separate data structures" reflective of some selected measure of network packets seen by a sensor, as opined by Dr. Kesidis. (Compare D.I. 266, ex. F at 72; D.I. 288, ex. F at 13-20) The court, therefore, finds that SRI has failed to demonstrate any genuine issue of material fact as to infringement of the '338 patent by Symantec's accused products. The accused products do not literally meet the "statistical profile" limitation. The court further finds that application of the doctrine of equivalents to the facts at bar would render the limitation meaningless[9] and, therefore, grants Symantec's motion for summary judgment in this regard as well.

ISS argues that its accused product, the Proventia ADS, does not meet the "receiving/receive network packets handled by a network entity" limitation.[10] ISS acknowledges that "[a]ll network packets that are transmitted over the internet are . . . 'handled by various network entities'" such as routers. (D.I. 399 at 16) ISS argues, however, that when Proventia ADS is operating in standalone or "Tap Mode," it is not linked to a

[9] Bicon, Inc. v. Straumann Co., 441 F.3d 945, 950-51 (Fed. Cir. 2006); Elekta Instrument S.A. v. O.U.R. Scientific Int'l, Inc., 214 F.3d 1302, 1305 and 1307 (Fed. Cir. 2000).

[10] This limitation was not construed by the court, as it was not identified as a disputed limitation by the parties.

network entity but, rather, receives network packets directly off the wire through its own tap. (D.I. 399 at 15-16; D.I. 294 at ¶ 8) The record indicates, however, that the "Tap Mode" is rarely used, meaning that the Proventia ADS is capable of infringing most of the time. Moreover, there is a genuine issue of material fact as to whether the traffic flowing on the wire between two network entities has been "handled" by a network entity. (See e.g., D.I. 336, ex. N at 6) Therefore, ISS's motion for summary judgment is denied in this regard.

ISS also argues that the Proventia ADS does not meet the "determining/determine" step of the asserted claims, because "[i]t does not calculate a difference between a short-term and long-term profile and, therefore, cannot determine anything about such a difference. Instead, the Proventia ADS computes the difference between current traffic activity and a composite measure of three different baselines - one based on a Day, one based on a Month and one that is Continuous." (D.I. 300 at 25) ISS's analysis is based on its proposed claim construction, which required that the difference "exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation between two profiles, requiring no prior knowledge of suspicious network activity." (Id.) The court did not adopt ISS's claim construction and, therefore, its motion is denied in this regard.

As its final argument, ISS contends that ADS does not infringe because it neither builds nor compares long-term and short-term statistical profiles. (D.I. 399 at 18-19) According to ISS, "[t]he values in the ADS baselines and snapshot[s] are average byte rates for the particular traffic filter. . . . These baselines and snapshots are not statistical profiles under any offered construction of profile. An average is not a statistical description . . . . Nor is the composite score calculated from these averages a statistical description . . . ." (Id., citing D.I. 294 at ¶ 11) The record indicates that there are genuine issues of material fact in this regard. (See D.I. 294 at ¶ 11; D.I. 336, ex. E at 27 ("[T]he PNADS method uses a fixed threshold to compare the short-term and long-term profiles.")) Therefore, ISS's motion for summary judgment is denied in this regard.

V. CONCLUSION

For the reasons stated, Symantec's motion for summary judgment of non-infringement (D.I. 286) is granted in part and denied in part. ISS's motion for summary judgment as it relates to non-infringement (D.I. 291) is denied.

An order shall issue.